INSTYTUT KOŚCIUSZKI | BRIEF PROGRAMOWY | STYCZEŃ 2020
ISSN 1689-9873

PRANIE PIENIĘDZY I FINASOWANIE TERRORYZMU

Z WYKORZYSTANIEM WALUT WIRTUALNYCH

dr Paweł Opitek – prokurator w Prokuraturze Krajowej,
ekspert ds. cyberprzestępczości i cyberbezpieczeństwa

Innowacje technologiczne od zawsze stanowiły koło napędowe cywilizacji, ale w ostatnim czasie obserwuje się skokowy postęp w zakresie implementacji nowych rozwiązań w przemyśle, medycynie i usługach. Oprócz niewątpliwych korzyści, zjawisko to generuje także nieznane wcześniej formy przestępczości z zastosowaniem metod i narzędzi teleinformatycznych, takich jak kryptografia, tokeny cyfrowe, anonimizacja ruchu sieciowego czy złośliwe oprogramowanie. Coraz popularniejsze stają się waluty i serwisy wirtualne służące do prania pieniędzy i wspierania terroryzmu, a w darknecie powstał rynek finansowy chętnie wykorzystywany przez cyberprzestępców. Łączy on w sobie tradycyjne usługi związane m.in. z pieniądzem elektronicznym i transferami bankowymi oraz płatnościami dokonywanymi kryptowalutą przy udziale platform cyfrowych typu giełdy i kantory wymiany walut wirtualnych. Jednak cyberprzestrzeń nie jest całkowicie odseparowana od tzw. realnego świata, bowiem aktywa „wyprane" z wykorzystaniem dostarczycieli usług sieciowych z reguły zamieniane są na pieniądz fiducjarny i wprowadzane do legalnego obrotu gospodarczego. Chociaż pełna skala omawianych nadużyć nie jest do końca znana, to szacuje się, że ogólnoświatowa wartość defraudacji z zaangażowaniem samych tylko kryptowalut w lipcu 2018 r. wyniosła co najmniej 7 mld euro. Amerykański Financial Crimes Enforcement Network (FinCEN) w maju 2019 r. raportował, że „przestępcy nadal wykorzystują wirtualną walutę do wspierania nielegalnej aktywności, prania pieniędzy i innych działań zagrażających bezpieczeństwu narodowemu Stanów Zjednoczonych"[1]. Mowa zatem o bardzo niebezpiecznym dla poszczególnych krajów i całej społeczności międzynarodowej obrazie przestępczości. Ma ona skomplikowany charakter i cały czas ewoluuje, co determinuje po stronie organów ścigania konieczność dostosowywania się do nowych uwarunkowań. Skoro waluty wirtualne są coraz częściej wykorzystywane jako alternatywa dla tradycyjnych systemów płatności i przekazów pieniężnych, to instytucje finansowe i publiczne ciała nadzorujące rynek powinny objąć obrót nimi efektywną kontrolą. Celem niniejszego opracowania jest ukazanie dwóch stron tego samego zjawiska: metod prania pieniędzy i finansowania terroryzmu za pomocą tokenów cyfrowych oraz przeciwdziałania wymienionym patologiom.

W niniejszym opracowaniu do określenia binarnych praw majątkowych zastosowano wymiennie różne nazewnictwo tj. waluty wirtualne, kryptowaluty, tokeny cyfrowe, bitmonety, cyfrowe prawa majątkowe. Chociaż zakresy znaczeniowe wymienionych pojęć nie są całkowicie tożsame, mają charakter niedookreślony, a ich interpretacja budzi spore kontrowersje, to jednak użycie przytoczonych określeń wymiennie nie miało zasadniczego wpływu na charakterystykę podjętego tematu.

1 *FinCen Guidance*, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf, data odczytu: 23.08.2019 r.

PRANIE PIENIĘDZY

Pranie pieniędzy polega na rozporządzaniu korzyściami finansowymi pochodzącymi z nielegalnej działalności w taki sposób, aby ukryć ich związek z czynem, w wyniku którego zostały uzyskane. Stanowi ono niejako akt wtórny w stosunku do przestępstwa bazowego[2], a ogólny model „prania" wygląda następująco:

1. nielegalnie uzyskane aktywa są zaangażowane w różnego rodzaju transakcje, często bez ekonomicznego uzasadnienia, celem „zaciemnienia" źródła ich pochodzenia;
2. wprowadzenie „wypranych" pieniędzy do oficjalnego systemu finansowego poprzez m.in. zamianę walut cyfrowych na pieniądz fiducjarny i zdeponowanie go na rachunku bankowym;
3. lokowanie wypranych środków w (pozornie) legalne inwestycje np. nieruchomości, przedsiębiorstwa czy tokeny cyfrowe.

Ściganie karne przestępstw związanych z praniem pieniędzy stanowi jeden z głównych priorytetów organów ochrony prawa na całym świecie, gdyż pozwala odbierać przestępcom korzyści pochodzące z nielegalnych działań, a bez możliwości wyprania pieniędzy realizacja czynów zabronionych jest dla nich nieopłacalna. Wynika z tego, że skuteczne zwalczanie „prania" ogranicza liczbę „bazowych" czynów zabronionych, takich jak handel narkotykami, wyłudzenia podatku VAT czy cyberprzestępczość ukierunkowana na sektor bankowy. Pieniądze pochodzące z nielegalnego źródła przeznaczane są zazwyczaj na luksusowe towary, inwestycje biznesowe, a ponadto do korumpowania urzędników, rozwijania przestępczej infrastruktury oraz wspierania autorytarnych ruchów i partii politycznych.

W polskim systemie prawnym legalna definicja „prania pieniędzy" znajduje się w art. 2. ust. 2 pkt 14) ustawy z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[3] (dalej: upp). Rozumie się przez to czyn określony w art. 299 ustawy Kodeks karny[4] (dalej: k.k.), który stanowi: „Kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące z korzyści związanych z popełnieniem czynu zabronionego, przyjmuje, posiada, używa, przekazuje lub wywozi za granicę, ukrywa, dokonuje ich transferu lub konwersji, pomaga do przenoszenia ich własności lub posiadania albo podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku, podlega karze pozbawienia wolności od 6 miesięcy do lat 8". Bez znaczenia dla zaistnienia przestępstwa jest postać technologiczna przedmiotu czynności wykonawczej. Jednostka kryptowaluty i inne tokeny cyfrowe jako prawa majątkowe mieszczą się w pojęciu „mienia", o którym mowa w art. 44 Kodeksu cywilnego[5]. Przedmiotem czynności wykonawczej przestępstwa prania pieniędzy są „prawa majątkowe lub inne mienie ruchome", a zatem mogą nim być również tokeny cyfrowe, jako owoc przestępstwa „bazowego" np. kryptowaluty uzyskane w wyniku ataku hakerskiego na wirtualną giełdę. Innym razem sprawca uzyska tokeny dopiero na późniejszym etapie „prania" np. kupując bitcoiny (BTC) za pieniądz fiducjarny. Realizacja znamion art. 299 k.k. nie wymaga podejmowania szczególnych działań, ale chodzi o wykazanie po stronie sprawcy zamiaru polegającego na ukryciu wspomnianych wartości.

Chociaż obecnie przestępstwa z art. 299 k.k. najczęściej realizowane są przy wykorzystaniu tradycyjnych instrumentów finansowych, to wraz z rozwojem walut wirtualnych pranie pieniędzy staje się poważnym problemem także w cyberprzestrzeni. W ciągu ostatnich lat pojawiło się wiele rodzajów wirtualnych praw majątkowych oraz narzędzi do zarządzania nimi. Równocześnie ewoluują różne modele biznesowe oparte na tokenach, których przykład stanowi tzw. ekonomia współdzielenia (ang. *sharing economy*).

> ***Sharing economy*** wykorzystano przy tokenizacji udziałów Regis Aspen Resort – luksusowego hotelu położonego w Kolorado (Stany Zjednoczone). Właściciel kurortu za pośrednictwem platform do crowdfundingu – Templum Markets i Indiegogo – sprzedał za 18 mln dolarów żetony AspenCoin, reprezentujące udziały w posiadłości, które w dalszej perspektywie mają współtworzyć ogólnoświatowy, wirtualny system obrotu nieruchomościami. AspenCoin w rozumieniu prawa amerykańskiego stanowią papiery wartościowe, a ich emisja podlegała rejestracji w amerykańskiej Komisji Papierów Wartościowych i Giełd (Securities and Exchange Commission, SEC). Na całym świecie powstaje obecnie wiele podobnych projektów opartych na technologii blockchain m.in. SwissRealCoin, Treehouse czy Resolute.Fund[6].

2 Według Konwencji Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu „przestępstwo bazowe" oznacza każde przestępstwo, wskutek którego zostały uzyskane dochody, które mogą być przedmiotem przestępstwa prania pieniędzy (J. Duży, Korzyść w przestępstwie prania pieniędzy, „Prokuratura i Prawo", nr 12, 2010).

3 Dz. U. 2019.1115 j. t.

4 Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r., Nr 88, poz. 553 z późn. zm.).

5 Ustawa z dnia 23 kwietnia 1964 roku Kodeks cywilny (Dz. U. 1964 Nr 16 poz. 93).

6 P. Opitek, Zastosowanie technologii blockchain na rynku nieruchomości, „Nieruchomości@", Kwartalnik Ministerstwa Sprawiedliwości, czerwiec 1/2019, s. 104.

FINANSOWANIE TERRORYZMU

Terroryzm można opisywać na różne sposoby. Podstawowa definicja określa terroryzm jako groźbę użycia przemocy lub jej gwałtowne użycie celem zastraszenia lub zranienia ludności albo spowodowania znacznych strat w mieniu dla korzyści politycznych lub ideologicznych. Chociaż Polska nie doświadczyła dotąd krwawych zamachów terrorystycznych, to stanowią one nad Wisłą realne zagrożenie. Sytuacja międzynarodowa powoduje, że w każdej chwili może dojść do ataku, co wynika m.in. z przynależności Polski do bloku państw walczących ze światowymi ekstremizmami, a więc narażonych na działania odwetowe terrorystów. Położenie geograficzne kraju sprawia, że jego granica wschodnia stanowi równocześnie linię strefy Schengen i przez Polskę przebiegają szlaki przerzutu osób i towarów z obszaru dawnego ZSRR oraz z Azji Centralnej i Południowo-Wschodniej do Europy Zachodniej. Najprawdopodobniej szlaki te są wykorzystywane przez osoby związane z ugrupowaniami terrorystycznymi.

W polskim k.k. zdefiniowano „przestępstwo o charakterze terrorystycznym" jako czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:

1. poważnego zastraszenia wielu osób,
2. zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
3. wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej

– a także groźba popełnienia takiego czynu (art. 115 § 20 k.k.).

Organizowanie działań o charakterze terrorystycznym wymaga wsparcia finansowego, a terroryści mogą otrzymywać taką pomoc w postaci cyfrowej. W kręgach fundamentalistów islamskich toczyła się dyskusja o tym, czy kryptowaluty są dozwolone przez szariat i czy muzułmanie powinni je wykorzystywać. Ostatecznie Al-Kaida opublikowała latem 2014 r. manifest pt. *Bitcoin wa Sadaqat al-Jihad: Bitcoin and the Charity of Violent Physical Struggle*[7] promujący użycie BTC jako dogodnego środka wsparcia walki z niewiernymi. Opisano w nim techniczne walory walut wirtualnych, takie jak odporność na fałszerstwa, anonimowość nadawców i odbiorców, globalny zasięg czy trudności w wykryciu płatności przez organy ścigania. Podkreślono wyższość systemu Bitcoina nad PayPal czy eBay, które zarządzane są odgórnie i mają charakter scentralizowany. Twórcom manifestu chodziło o stworzenie całkowicie anonimowego systemu do wysyłania darowizn w BTC o wartości milionów dolarów na adres portfela „DarkWallet" (portfel rzeczywiście pojawił się w darknecie w 2019 r.) czy zakupu broni. W konkluzji autorzy manifestu stwierdzili, że chociaż wykorzystanie bitcoina natrafia na różne przeszkody, a „większość kafirów używała go do nabycia narkotyków"[8], to jednak posiada w sobie duży potencjał. Pokłosiem tego było pojawienie się wielu kont w mediach społecznościowych organizujących zbiórki w kryptowalucie na rzecz terrorystów islamskich z różnych krajów i organizacji.

Zgodnie z art. 2. ust. 2 pkt 6) upp przez „finansowaniu terroryzmu" rozumie się czyn określony w art. 165a k.k.: karze pozbawienia wolności od lat 2 do 12 podlega ten, kto gromadzi, przekazuje lub oferuje środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości w zamiarze sfinansowania przestępstwa o charakterze terrorystycznym lub innego enumeratywnie wymienionego w ustawie poważnego przestępstwa (np. stosowania środków masowej zagłady).

Trudno na chwilę obecną jednoznacznie oszacować, jakie środki w walucie cyfrowej otrzymali terroryści islamscy. Wiele wskazuje na to, że np. sprawcy zamachów terrorystycznych przeprowadzonych 13 listopada 2015 r. w Paryżu, byli wspierani przekazami kryptowalutowymi[9]. Faktem jest, że środowiska wspierające finansowanie islamskiego terroryzmu stosują socjotechnikę, a prowadzone przez nich zbiórki mają profesjonalny charakter. W trakcie kampanii prowadzonej pod hasłem „Wyposażcie Nas!" w lipcu 2016 r. przez Ibn Taymiyya Media Center (internetową jednostkę medialną Rady Mudżahedinów „Szura") zachęcano do wysyłania darowizn w BTC, podając szczegółową instrukcję, jak realizować przelewy kryptowalutowe[10]. Z drugiej strony w ciężkich warunkach frontowych zapewne bardziej sprawdza się tradycyjny pieniądz, aniżeli bitmonety zgromadzone w aplikacji elektronicznej. Krąg osób obeznanych w funkcjonowaniu cyfrowych wartości majątkowych także jest stosunkowo nieliczny. Dochodzi do tego nieufność użytkowników sieci i ich wątpliwości, kto jest rzeczywistym administratorem zbiórki i co dzieje się ze środkami zgromadzonymi na podanym adresie portfela.

7 Taqi'ulDeen alMunthir, *Bitcoin wa Sadaqat alJihad: Bitcoin and the Charity of Violent Physical Struggle*, https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf, data odczytu: 20.01.2019 r.

8 Ibidem.

9 Zob. m.in. https://www.coindesk.com/bitcoin-paris-and-terrorism-what-the-media-got-wrong.

10 P. Opitek, *Cyberprzestępczość w pracy prokuratora*, Wydawnictwo Prokuratura i Prawo. Wydanie Specjalne, Prokuratura Krajowa 2018 r., s. 23.

Przypadki konkretnych działań terrorystycznych zależą od wielu czynników m.in. motywującej je ideologii, postawy, celów i kompetencji poszczególnych osób czy przedsięwziętej taktyki. W odniesieniu do taktyki „samotnego wilka" i małych komórek zasoby finansowe potrzebne do przeprowadzenia ataku są dość niskie np. terrorysta atakujący w Nicei w 2016 r. potrzebował niewielkich funduszy na wynajęcie ciężarówki i najbezpieczniej było zapłacić za nią gotówką lub kartą kredytową. Jeśli chodzi o większe grupy (Al-Kaida, ISIS), to jest mało prawdopodobne, aby mogły całkowicie oprzeć finansowanie podejmowanych operacji na walutach cyfrowych. Przykładowo, sponsorowanie działalności Państwa Islamskiego w Syrii i Iraku dotyczyło przede wszystkim egzekwowania opodatkowania osób fizycznych i przedsiębiorstw znajdujących się pod jego kontrolą. Jednak sytuacja stale się zmienia i nawet jeśli dzisiaj operowanie cyfrowymi walutami pozostaje działalnością marginalną wśród dżihadystów, to terroryści islamscy adaptują się do nowej rzeczywistości i podejmują próby wykorzystania innowacyjnych technologii finansowych na coraz większą skalę.

Ali Shukri Amin mieszkał w Virginii, gdzie podczas studiów zaczął się radykalizować, a swoje poglądy propagował w mediach społecznościowych. Na swoim koncie Twitter o nazwie @AmreekiWitness zamieścił 7000 tweetów propagujących radykalny islam i namawiających do wsparcia finansowego ISIS za pomocą anonimowych transferów bitcoinowych. Prowadził także blog „Al-Khilafah Aridat" zachęcający do walki z „niewiernymi", na którym zamieszczał artykuły szczegółowo opisujące, jak anonimowo komunikować się w sieci i stosować szyfrowanie w nielegalnej aktywności na rzecz terrorystów. W 2015 r. prokurator skierował do sądu akt oskarżenia[11] przeciwko Ali Shukri Amin zarzucając mu angażowanie się w działalność terrorystyczną, polegającą na udzieleniu wsparcia materialnego i fachowych porad zagranicznym terrorystom z ISIS. Mężczyzna został skazany przez sąd na długoletnią karę pozbawienia wolności.

Waluty cyfrowe pozostają ponadto w obszarze zainteresowania państw, które z powodu nałożonych sankcji mają ograniczone możliwości korzystania z globalnego systemu finansowego m.in. w zakresie realizacji transakcji pieniądzem elektronicznym oraz uzyskiwania kredytów i pożyczek. Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy (The Financial Action Task Force, FATF) wielokrotnie podkreślała swoje zaniepokojenie sytuacją w Republice Iranu i Koreańskiej Republice Ludowo-Demokratycznej (KRLD).

11 CRIMINAL NO. 1:15-CR-164, Defendant's memorandum in aid of sentencing, https://www.investigativeproject.org/documents/case_docs/2826.pdf, data odczytu: 23.08.2019 r.

FATF wezwała KRLD do natychmiastowego zajęcia się brakiem efektywnej polityki przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT) i związaną z tym nielegalną działalnością w zakresie proliferacji broni masowego rażenia i jej finansowaniem[12]. W ostatnich latach wiele cyberataków inicjowanych było z terenu Korei Północnej w celu uzyskania kryptowaluty na sponsorowanie tamtejszego reżimu. Chodzi m.in. o dokonane w 2017 r. ataki złośliwego oprogramowania typu ransomware o nazwie WannaCry, którym zainfekowano ćwierć miliona komputerów na całym świecie. Wirus szyfrował pliki i żądał zapłaty okupu w BTC za ich odszyfrowanie. Cyfrowe ślady działania złośliwego kodu prowadziły do hakerskiej grupy Lazarus powiązanej z rządem Korei Północnej. Stany Zjednoczone oficjalnie przypisały temu państwu odpowiedzialność za ataki.

Departament Skarbu Stanów Zjednoczonych ds. Kontroli Aktywów Zagranicznych (Office of Foreign Assets Control, OFAC) w listopadzie 2018 r. podjął działania przeciwko dwóm Irańczykom – Ali Khorashadizadeh i Mohammadowi Ghorbaniyanow – którzy pomagali wymieniać bitcoiny na riale, a następnie deponowali pieniądze na rachunkach irańskich banków. Kryptowaluta została uzyskana jako zapłata „cyfrowego" okupu w prowadzonych od 2015 r. atakach złośliwego oprogramowania typu ransomware o nazwie SamSam ukierunkowanego na komputery ponad 200 korporacji, szpitali, uniwersytetów i agencji rządowych ze Stanów Zjednoczonych, Wielkiej Brytanii i Kanady. OFAC zidentyfikował dwa adresy BTC[13] powiązane z ww. przestępcami, które uczestniczyły w ponad 7000 transakcjach dotyczących przesłania wartych miliony dolarów bitcoinów[14].

Iran to kolejny kraj, którego system prawny posiada duże braki w implementacji międzynarodowych standardów dotyczących AML/CFT. FATF wobec Republiki ajatollahów od dawna stosuje tzw. środki zaradcze, ale też oferował pomoc techniczną w celu wdrożenia działań naprawczych. W rezultacie sektor finansowy Iranu stał się bezpieczniejszy dzięki m.in. uchwaleniu poprawek w sierpniu 2018 r. do ustawy o walce z finansowaniem terroryzmu oraz w styczniu 2019 r. do ustawy o przeciwdziałaniu praniu pieniędzy. Jednak Iran powinien jeszcze efektywniej zająć się

12 Publiczne oświadczenie FATF – czerwiec 2019 r., https://www.gov.pl/web/finanse/publikacje-fatf, data odczytu: 23.08.2019 r.

13 Chodzi o adresy: 49w62rY42aZBox8fGcmqNsXUzSStKeq8C oraz 1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V.

14 Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses, U.S. Department of the Treasury, November 28, 2018, https://home.treasury.gov/news/press-releases/sm556, data odczytu: 23.08.2019 r.

m.in. skuteczną kryminalizacją finansowania terroryzmu oraz wzmocnieniem weryfikacji przelewów bankowych pod kątem źródła pochodzenia środków[15].

CYFROWE PRAWA MAJĄTKOWE

W dokumentach organizacji międzynarodowych znajdują się różne definicje walut wirtualnych, które stanowią o wiele szerszy zbiór desygnatów, aniżeli pojęcie „kryptowaluta". W raporcie z 2015 r. Europejski Bank Centralny określił wspomniane waluty jako cyfrowe reprezentacje wartości, które nie zostały wydane przez bank centralny, instytucję kredytową lub instytucję pieniądza elektronicznego, nadające się w pewnych okolicznościach do wykorzystania jako alternatywa dla pieniędzy[16]. FATF używa terminu *Virtual Asset* (VA, wirtualne mienie), który definiuje jako cyfrową reprezentację wartości, która może być przedmiotem wirtualnego handlu lub transferu i którą można realizować płatności lub cele inwestycyjne[17]. *Virtual Asset* nie są: cyfrowe postacie pieniądza, papierów wartościowych lub innych instrumentów finansowych. Przytoczona definicja jest istotna choćby dlatego, że kraje implementujące rekomendacje FATF do własnego porządku prawnego powinny ją respektować.

Instytucje nadzorujące rynek różnie określają cyfrowy majątek. Brytyjski Financial Conduct Authority (FCA) w opracowaniu pt. *Guidance on Cryptoassets*[18] tytułową nazwę „cryptoassets" przypisuje cyfrowej reprezentacji wartości lub zobowiązaniu umownemu opartemu na kryptograficznym bezpieczeństwie wynikającym z różnych form technologii rozproszonych rejestrów, które mogą być elektronicznie gromadzone, przesyłane i podlegają obrotowi handlowemu. W dokumentach FinCEN-u zbiorczą nazwą CVC (ang. *convertible virtual currency*) określa się: walutę cyfrową (ang. *digital currency*), kryptowaluty (ang. *cryptocurrency*), wartości oparte na kryptografii (ang. *cryptoasset*) oraz aktywa cyfrowe (ang. *digital asset*). Brak jednej definicji cyfrowych wartości majątkowych wynika z faktu, że na świecie funkcjonują dziesiątki tysięcy tokenów, które różnią się nie tylko nazwą, ale przede wszystkim statusem prawno-ekonomicznym.

PODSTAWOWY PODZIAŁ WYRÓŻNIA NASTĘPUJĄCE GRUPY BINARNYCH ŻETONÓW:

1. **tokeny wymienne** (ang. *exchange tokens*): skonstruowane jako środek wymiany, a obrót nimi jest zdecentralizowany. Służą do zapłaty za towary i usługi, podobnie jak inne dobra materialne, którym nadaje się określoną wartość w obrocie międzynarodowym. Opisane tokeny znajdują się zazwyczaj poza systemem regulacyjnym: np. w Anglii kupno, sprzedaż lub obrót *exchange tokens* nie jest regulowany przez Komisję Nadzoru Finansowego (Financial Conduct Authority) (dotyczy to także komercyjnej działalności polegającej na prowadzeniu kantorów);
2. **tokeny stanowiące papiery wartościowe** (ang. *security tokens*): spełniają funkcję papierów wartościowych lub innych instrumentów finansowych i przeznaczone są do celów inwestycyjnych oraz podlegają szczegółowym przepisom regulacyjnym;
3. **tokeny użytkowe** (ang. *utility tokens*): ich posiadacz ma prawo dostępu do aktualnego lub mającego pojawić się w przyszłości produktu lub usługi. Jednocześnie nie inkorporują praw i obowiązków podobnych do *security tokens*, chociaż w pewnych okolicznościach mogą pełnić rolę pieniądza elektronicznego (ang. *e-money*) i wtedy ich użytkowanie wymaga stosownej licencji lub pozwolenia[19].

Praktyczne znacznie ma określenie statusu prawnego konkretnych tokenów, szczególnie odpowiedź na pytanie o to, czy są one instrumentami finansowymi, bowiem od tego zależą prawa i obowiązki uczestnika rynku, który nimi dysponuje. Co do zasady to właściciel/posiadacz/zarządca tokena powinien znać jego naturę i spełniać wymogi z niej wynikające, związane np. z obowiązkiem uzyskania zgody na emisję cyfrowych jednostek lub raportowania o obrocie nimi. Ponieważ brak w tym zakresie orzeczeń sądów polskich oraz pogłębionych opracowań krajowych instytucji finansowych, warto przytoczyć dwa zagraniczne stanowiska – brytyjskiej Komisji Nadzoru Finansowego oraz amerykańskiej Komisji Papierów Wartościowych i Giełd.

FCA wskazuje[20], że token stanowi instrument finansowy (ang. *specified investment*) jeśli:

- jego posiadacz/właściciel ma z tego tytułu sprecyzowane prawa i obowiązki o charakterze zobowiązaniowym (np. prawo do dywidendy);

15 Publiczne Oświadczenie FATF – czerwiec 2019 r...., op. cit.

16 *Virtual currency schemes – a further analysis*, European Central Bank, February 2015, s. 25, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, data odczytu: 12.08.2018 r.

17 *Virtual Assets and Virtual Asset Service Provider*, Guidance for a risk-based approach, FATF 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf., s. 13.

18 *Guidance on Cryptoassets, FCA Financial Conduct Authority*, Consultation Paper CP19/3, January 2019, s. 8.

19 Tamże, s. 8-9.

20 Tamże, s. 20-21.

- jednostki są określane (np. w folderze promocyjnym) mianem papierów wartościowych lub sugeruje się, że pełnią taką funkcję;
- token może być przenoszony (ang. *transferable*) oraz stanowić przedmiot obrotu (ang. *tradeable*) na platformach handlowych;
- zachodzi bezpośredni przepływ płatności pomiędzy emitentem tokenów i ich posiadaczem.

W Stanach Zjednoczonych umowy inwestycyjne muszą być zgodne zarówno z ustawą o papierach wartościowych z 1933 r., jak i ustawą o giełdzie papierów wartościowych z 1934 r. Podmioty oferujące sprzedaż papierów wartościowych zobowiązane są do przestrzegania federalnych przepisów dotyczących takich instrumentów, w tym wymogu rejestracji przedsięwzięcia w SEC lub uzyskania stosownego zwolnienia. Ponadto podmiot lub osoba prowadząca działalność giełdową powinna zarejestrować się jako krajowa giełda papierów wartościowych oraz złożyć oświadczenie i prospekt emisyjny. Naruszenie wspomnianych wymagań prowadzi do odpowiedzialności cywilno-administracyjnej.

Obowiązek rejestracyjny dotyczy emitenta papierów wartościowych niezależnie od tego, czy działa w formie tradycyjnej spółki prawa handlowego, czy chodzi o zdecentralizowaną organizację cyfrową. Nie ma znaczenia, czy cena za akcje wyznaczona jest w dolarach, czy cyfrowych tokenach oraz czy akcje są dystrybuowane w postaci „papierowych" certyfikatów inwestycyjnych, czy poprzez technologię rozproszonej księgi. Podsumowując, to, czy dana transakcja wiąże się z ofertą i sprzedażą papierów wartościowych zależy od prawno-ekonomicznej konstrukcji *smart contracts*, a terminologia użyta w „białej księdze" ma znaczenie drugorzędne.

W orzecznictwie sądów amerykańskich zostały wypracowane „testy" do oceny, czy dany projekt jest umową inwestycyjną i spowoduje emisję papierów wartościowych. Najpopularniejszy jest Test Howeya, w ramach którego transakcja jest umową inwestycyjną jeżeli:

- osoba inwestuje swoje pieniądze;
- inwestor oczekuje zysków z inwestycji;
- inwestowanie pieniędzy odbywa się we wspólne przedsięwzięcie inwestujących osób i emitentów tokenów;
- wszelkie zyski z inwestycji są rezultatem wysiłków podejmowanych przez organizatora inwestycji lub podmiot trzeci.

Komisja Papierów Wartościowych i Giełd przyjmuje, że Test Howey'a stosuje się także do przedsięwzięć opartych na tokenach ponieważ rozwój rynków kapitałowych i nowych technologii rozszerzył inicjatywy biznesowe o inwestycje w cyfrowe prawa majątkowe.

Art . 2 ust. 2 pkt 26) upp stanowi: Waluta wirtualna – rozumie się przez to cyfrowe odwzorowanie wartości, które nie jest:

a. prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,

b. międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,

c. pieniądzem elektronicznym w rozumieniu ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych,

d. instrumentem finansowym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,

e. wekslem lub czekiem

– oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego.

W prawie polskim legalna definicja walut wirtualnych znajduje się w art. 2 ust. 2 pkt 26) upp. Pojawiły się głosy krytyczne wobec jej kształtu z uwagi na zbyt szerokie i niejednoznaczne określenie przedmiotu definiowanego, co powodować może trudności w precyzyjnej kwalifikacji stanu faktycznego konkretnej sprawy karnej. Podzielając pogląd, że wspomniany przepis może rodzić problemy w procesie stosowania prawa, to jednak należy przyznać, że nie sposób skonstruować prostej i jednoznacznej definicji „walut wirtualnych" wobec różnorodnego charakteru prawnego tysięcy tokenów i ich różnych funkcji użytkowych. Niemniej przepis art. 2 ust. 2 pkt 26) upp stanowi znaczące usystematyzowanie przedmiotu definiowanego, a nadanie konkretnego sensu terminowi „waluty wirtualne" nastąpi w procesie wykładni i stosowania prawa z uwzględnieniem doktryny prawniczej i orzecznictwa sądowego.

CECHY WALUT CYFROWYCH SPRZYJAJĄCE PRZESTĘPCZOŚCI

Cechy wirtualnych tokenów powodują, że wykorzystywane są do popełniania przestępstw. W pierwszej kolejności oferują one o wiele większą aniżeli w przypadku kart płatniczych i innych produktów oferowanych przez tradycyjną bankowość anonimowość transakcji. Z uwagi na najszerszy krąg użytkowników, wciąż najpopularniejszy w cyberprzestępczości jest bitcoin. Jego architektura nie zawiera informacji o osobach/podmiotach realizujących operacje kryptowalutowe, jednak umieszczone na blockchainie rekordy transakcji w BTC dostarczają pewnych informacji, a na rynku dostępne są coraz skuteczniejsze narzędzia do śledzenia przepływów bitcoinowych. Dlatego przestępcy coraz częściej sięgają po inne bitmonety, typu Monero, Dash lub Zcash, ukrywające także wielkości, czas i miejsce realizacji transferów. Pozostałe cechy walut wirtualnych, sprzyjające cyberprzestępczości, to:

- nieporównywalnie krótszy czas realizacji (szczególnie międzynarodowych) przelewów, niż tradycyjnych transferów gotówkowych;
- powszechna akceptowalność walut wirtualnych w podziemiu przestępczym;
- lokalizacja serwisów internetowych w jurysdykcjach pozbawionych skutecznych mechanizmów przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu;
- częsty brak centralnego administratora zarządzającego transakcjami, co powoduje trudności w egzekwowaniu obowiązków AML/CFT.

Rynek VA znajduje się w cyberprzestrzeni co oznacza, że sprawowanie nad nim kontroli jest mniej efektywne, aniżeli nad sprawdzonymi instytucjami typu banki czy giełdy towarowe. Zdarza się, że sami uczestnicy wirtualnego rynku nie wiedzą do końca, jaki charakter prawny ma oferowany przez nich produkt lub usługa stanowiące zupełne *novum* w świecie finansów. Nowa, nierozpoznana do końca natura cyfrowych żetonów zwiększa ryzyko malwersacji i daje sposobność do prania pieniędzy. Sprzyja temu brak spójnego, globalnego nadzoru nad podmiotami świadczącymi usługi oraz odmienne regulacje prawne szczególnie w miejscach, gdzie brak skutecznych procedur AML/CFT pozwala uniknąć obowiązków regulacyjnych, standardów związanych z uzyskaniem stosownych zezwoleń na prowadzenie działalności i raportowaniem podejrzanych transakcji.

Przestępcy wypracowali i cały czas udoskonalają metody prania pieniędzy w Internecie. W przypadku kryptowalut chodzi m.in. o tworzenie wielu nowych adresów dla każdego przychodzącego przelewu i kreowanie fikcyjnych użytkowników kryptowalut, wykorzystywanie sieci TOR i VPN-ów, stosowanie specjalnych serwisów sieciowych do „zacierania" historii bitmonet, rozdrabnianie sald walut cyfrowych, a następnie korzystanie z aplikacji do konsolidowania wielu bitcoinowych adresów w jednym portfelu do zarządzania nimi z każdego urządzenia (ang. *third-party eWallet service*)[21].

Inne symptomatyczne działania mogące świadczyć o procederze prania pieniędzy, to:

- duża liczba rachunków bankowych należąca do jednego administratora walut cyfrowych (tzw. konta rozwarstwione);
- sytuacja, gdy bitcoinowe firmy mają siedzibę w jednym kraju, ale zakładają rachunki za granicą bez logicznego uzasadnienia takiej aktywności;
- przepływy jednostek kryptowaluty pomiędzy wieloma rachunkami zlokalizowanymi w odmiennych jurysdykcjach i przypisanymi do różnych podmiotów;
- duża liczba i znaczna częstotliwość niskich kwotowo operacji gotówkowych lub „krypto"[22].

Sygnały prowadzenia nielegalnej działalność, zauważalne od strony dostarczycieli usług do zarządzania cyfrowymi prawami majątkowymi (ang. *virtual asset service provider*, VASP), to:

- inicjowanie transakcji z adresów IP przypisanych krajom objętym sankcjami lub IP uprzednio wykorzystanych do popełniania przestępstw;
- wielokrotne konwersje między różnymi typami VA bez sprecyzowanego celu biznesowego;
- rozbieżności między adresami IP powiązanymi z profilem klienta, a adresami IP, z których inicjowane są transakcje;
- użytkownik platformy nie spełnia lub nie poddaje się weryfikacji w ramach procedury KYC (ang. *know your customer*);
- nagłe, nietypowe zachowania klienta, odbiegające od jego „profilu finansowego";
- adres portfela jest współdzielony między kontami należącymi do różnych osób;
- uczestnik platformy wielokrotnie zmienia adres e-mail, numer telefonu i inne dane osobowe[23].

21 *Bitcoin Virtual Currency: Intelligence Unique Features: Present Distinct*, Challenges for Deterring Illicit Activity, FBI Directorate of Intelligence, 24 April 2012, s. 5.

22 D.M. Sat, G.O. Krylov, K. Evgenyevich, B. Bezverbnyi, A.B. Kasatkin, I.A. Kornev, *Investigation of money laundering methods through cryptocurrency*, Journal of Theoretical and Applied Information Technology, January 2016, Vol. 83, No. 2, s. 245–246.

23 *Advisory on Illicit Activity Involving Convertible Virtual Currency*..., op. cit., s. 9-10.

Pojawiają się plany budowy systemu ścisłego monitorowania transakcji kryptowalutowych w celu powstrzymania przepływu środków na nielegalne przedsięwzięcia. Pracuje nad nim m.in. 15 państw, w tym członkowie G7, pod egidą FATF. System ma zostać uruchomiony w 2020 roku i zakłada się, że wymiana kryptowalut każdorazowo będzie wymagała ścisłego potwierdzenia tożsamości klientów i bezpiecznego przechowywania tych informacji[24]. Trudno jednak przypuszczać, aby udało się wprowadzić mechanizm poddający rzeczywistej kontroli cały rynek wirtualnych usług.

ORGANY ZAANGAŻOWANE

Na świecie działają międzynarodowe instytucje i agencje, których zadaniem jest przeciwdziałanie praniu pieniędzy i zwalczanie terroryzmu, a czołowe miejsce w tym systemie zajmuje FATF. Instytucja ta utworzona została przez Międzynarodowy Fundusz Walutowy w 1989 r. i skupia 35 krajów członkowskich oraz 2 organizacje regionalne. Grupa za cel stawia sobie ustanowienie standardów i promowanie skutecznego wdrażania środków prawnych, regulacyjnych i operacyjnych do zwalczania prania pieniędzy, finansowania terroryzmu i innych poważnych zagrożeń dla integralności globalnego systemu finansowego. FATF jest zatem „organem doradczym", który działa na rzecz osiągnięcia niezbędnej woli politycznej i wprowadzenia reform legislacyjnych i regulacyjnych w obszarze AML/CFT na poziomie poszczególnych krajów. Obecnie jednym z głównych celów Grupy jest rozwiązanie problemu anonimowości w Internecie, jako narzędzia do prania pieniędzy za pośrednictwem wirtualnej waluty.

The Financial Action Task Force wypracował rekomendacje, które powinny być implementowane przez państwa celem zapobiegania i zwalczania przestępczości przy uwzględnieniu indywidualnych warunków, posiadanych już środków prawnych, własnych możliwości regulacyjnych i operacyjnych. Rekomendacje nakładają szereg obowiązków dotyczących:

- oceny i ograniczenia ryzyka związanego z aktywami wirtualnymi i dostawcami usług do ich obsługi;
- licencjonowania lub rejestrowania dostawców;
- nadzorowania i kontroli VASP przez właściwe organy krajowe (obowiązuje zakaz oddawania tych kompetencji organom samorządu zawodowego);
- wdrożenia sankcji w sytuacji, gdy usługodawcy nie przestrzegają zobowiązań AML/CFT;
- udoskonalania efektywności współpracy krajowej i międzynarodowej oraz partnerstwa publiczno-prywatnego;
- prowadzenia rejestrów, zgłaszania podejrzanych operacji i kontroli wszystkich transakcji pod kątem zgodności z przepisami;
- obowiązki dotyczą również koordynacji przepisów AML/CFT z innymi regulacjami, m.in. dotyczącymi ochrony danych i prywatności[25].

Rekomendacje FATF wymagają, aby członkowie Grupy zobowiązali dostawców usług do oceny oraz minimalizowania ryzyka dotyczącego prania pieniędzy i finansowania terroryzmu oraz wdrażania środków przeciwdziałających przestępstwom. Państwa mogą nawet zdelegalizować konkretne VA na podstawie własnej oceny ryzyka i własnego kontekstu regulacyjnego. Oprócz odgórnych regulacji, poszczególne rządy podejmują różnego rodzaju własne inicjatywy wzmacniające wewnętrzny system walki z malwersacjami. W Stanach Zjednoczonych przyjęto w 2019 r. ustawę o ochronie technologii finansowych (*The Financial Technology Protection Act*), której celem jest utworzenie grupy zadaniowej składającej się z przedstawicieli różnych agencji zajmującej się zwalczaniem nielegalnego wykorzystania kryptowaluty do wspierania terroryzmu.

> W jednym ze śledztw członkowie zorganizowanej grupy przestępczej umieszczali w Internecie fikcyjne oferty sprzedaży sprzętu budowlanego i rolniczego. Osoby zainteresowane nabyciem maszyn wpłacały wysokie zaliczki na poczet zawarcia umowy sprzedaży ciągnika czy dźwigu. Kwoty przelane na rachunek bankowy przestępców momentalnie transferowano na giełdę kryptowalutową i zamieniano na BTC. Dzięki podjętym działaniom, środki na giełdzie udało się zablokować, a następnie stały się one przedmiotem tymczasowego zajęcia mienia ruchomego dokonanego przez Policję. W ustawowym terminie prokurator wydał postanowienie o zabezpieczeniu majątkowym. Działania takie pozwalają m.in. na zwrot środków utraconych w wyniku przestępstwa osobom pokrzywdzonym.

Polskie organy ochrony prawa także przeciwdziałają nielegalnemu wykorzystaniu walut wirtualnych, a jednym z najskuteczniejszych środków jest pozbawianie sprawcy owoców przestępstwa. Podstawy prawne i techniczne realizacji tymczasowego zajęcia mienia ruchomego i zabezpieczenia majątkowego na cyfrowych prawach majątkowych zostały usystematyzowane w wydanej przez Prokuraturę Krajową

24 D. Palmer, *15 Nations Plan Global Crypto Monitoring System Under FATF: Report*, https://www.coindesk.com/, data odczytu: 23.08.2019 r.

25 Oświadczenie w sprawie wirtualnych aktywów i dostawców usług wirtualnych aktywów, https://www.gov.pl/web/finanse/publikacje-fatf, data odczytu: 23.08.2019 r.

Metodyce zabezpieczeń majątkowych[26]. Opisano w niej m.in. czynności zmierzające do zajęcia walut cyfrowych, sposób ich przechowywania na potrzeby śledztwa, a wszystko po to, aby stworzyć skuteczne mechanizmy realizacji zabezpieczenia majątkowego na kryptowalutach. Już dzisiaj cyfrowe tokeny przejmowane są w prowadzonych postępowaniach karnych. Nie mniej ważne jest zacieśnianie współpracy na omawianym polu, czemu służyła zorganizowana przez Prokuraturę Krajową w październiku 2019 r. w Katowicach międzynarodowa konferencja pt. „Kryptowaluty w cyberprzestępczości. Międzynarodowa wymiana doświadczeń".

PODMIOTY OBOWIĄZANE

Szczególna rola w rozpoznawaniu i blokowaniu nielegalnych transakcji wykorzystujących tokeny cyfrowe przypada dostarczycielom usług związanych z walutami cyfrowymi określanymi zbiorczą nazwą *Virtual Asset Service Provider*. VASP to każdy podmiot, który we własnym imieniu lub na rzecz osoby trzeciej prowadzi wymianę VA na pieniądze i odwrotnie, uczestniczy w transferach wirtualnych tokenów, zarządza lub administruje nimi oraz świadczy usługi finansowe powiązane z oferowaniem/sprzedażą VA lub wspiera podmioty, które oferują takie usługi[27]. VASP mogą funkcjonować w różnych formach i modelach biznesowych. Za VASP uznać należy m.in. wirtualne kantory wymiany tokenów cyfrowych czy podmioty zarządzające portfelami kryptowalutowymi i niektórych dostarczycieli takich portfeli „podpiętych" pod wirtualne giełdy z potencjałem realizacji transferów. Status VASP posiadają serwisy emitujące własne lub oferujące cudze tokeny lub zajmujące się sprzedażą jakichkolwiek cyfrowych praw majątkowych. Dostarczycielem usług związanych z obowiązkiem raportowania będzie również właściciel/administrator bankomatu kryptowalutowego, a także podmioty świadczące usługi przyjmowania zleceń na zakup i sprzedaż VA, które w ten sposób łączą potencjalne strony przyszłych transakcji, ustalając ich przedmiot i cenę, a finalnie udostępniając platformę do realizacji operacji (ang. *order-book exchange services*)[28]. Do VASP należy zaliczyć osobę fizyczną, która profesjonalnie trudni się wymianą walut cyfrowych na pieniądze „z ręki do ręki". Nie ma zatem znaczenia, czy płatności za usługi i inne transfery danych dokonywane są gotówką, przelewami bankowymi, kartami płatniczymi, tokenami cyfrowymi itp. Obowiązuje zasada „neutralności technologicznej", która oznacza, że ocenie podlega funkcja, jaką dany podmiot wykonuje na rynku bez względu na wykorzystywaną do tego technologię i infrastrukturę.

Odpowiedź na pytanie, czy dany podmiot ma status VASP uzależniona jest od tego, jak używa cyfrowych aktywów i kto jest beneficjentem świadczonych przez niego usług. Jeśli podmiot prowadzi aktywność opisaną w definicji VASP we własnym imieniu lub reprezentując „podmiot trzeci", to podlega określonym obowiązkom niezależnie od tego, czy stosuje w handlu platformę scentralizowaną, zdecentralizowaną, *smart contracts*, czy jeszcze inną technologię. Z drugiej strony, jeśli czynności angażujące waluty wirtualne są realizowane okazjonalnie przez „nie-przedsiębiorcę", np. płatności za zakupione do celów konsumpcyjnych towary w Internecie, to kupujący nie podlega pod definicję *Virtual Asset Service Provider*.

Ocena, czy podlega się pod reżim prawny dedykowany VASP zależy także od jurysdykcji, w której podmiot funkcjonuje. Państwa różnie kwalifikują dostarczycieli usług wirtualnych i nakładane na nich obowiązki, chociaż członkowie FATF powinni realizować w taki sam sposób rekomendacje przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Rozbieżności na omawianym polu są niepożądane i dlatego w dokumentach FATF zaleca się stosowanie podejścia funkcjonalnego: chociaż kraje modelują szczegółowe rozwiązania prawne pod kątem ich wewnętrznych, specyficznych uwarunkowań, to jednak implementacja zasadniczych wytycznych powinna wszędzie stać na niezmiennie wysokim poziomie.

Rekomendacje FATF mają pomóc instytucjom państwowym i podmiotom prywatnym zrozumieć zagrożenia wynikające z rozwoju rynku cyfrowych praw majątkowych oraz wprowadzać/rozwijać regulacje przeciwdziałające nadużyciom. FATF w formułowanych rekomendacjach wymaga od regulatorów:

- oszacowanie poziomu ryzyka związanego z funkcjonowaniem podmiotów związanych z rynkiem walut wirtualnych;
- nadzorowania i monitorowania ich działalności pod kątem przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu;
- określenia, jaki zakres działalności powinien być obwarowany uzyskaniem od organu państwowego stosownej rejestracji, pozwolenia lub licencji;
- nałożenia i egzekwowania od VASP obowiązku przechowywania historii transakcji;
- efektywnego raportowania przez podmioty obowiązane „podejrzanych" operacji;
- określenia sankcji grożących za niewywiązywanie się z obowiązków określonych przez przepisy AML/CFT.

Ponieważ cyberprzestrzeń, w której operują VASP i waluty wirtualne, pozbawiona jest granic i ma charakter ogólnoświatowy, to niezbędna jest współpraca międzynarodowa w zwalczaniu opisywanych zagrożeń. Chodzi m.in. o ustanowienie kompatybilnych przepisów prawnych ukierunkowanych

26 Metodyka przeznaczona jest do wewnętrznego użytku przez prokuraturę. Zob. także: P. Opitek, *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, Prokuratura i Prawo 2017/6, s. 36 i nast.

27 *Virtual Assets and Virtual Asset Service Provider*..., op. cit., s. 13-14.

28 Tamże, s. 14-15.

na przeciwdziałanie praniu pieniędzy i zwalczanie terroryzmu na całym świecie, a przynajmniej w państwach demokratycznych. Zalecenia FATF wymagają zatem od krajowych decydentów nałożenia na uczestników rynku walut cyfrowych określonych zobowiązań prawnych, chociaż każde państwo może skonkretyzować je w sposób odpowiadający własnemu porządkowi prawnemu.

PLATFORMY SŁUŻĄCE DO REALIZACJI PRZESTĘPSTW

Darkmarkety

Darkmarkety to platformy, na których znajdują się oferty sprzedaży nielegalnych towarów i usług. Działają one w tzw. ukrytym Internecie (ang. *darknet*), którego eksploracja możliwa jest dzięki wyszukiwarkom typu TOR Browser i specjalnemu oprogramowaniu. Darkmarkety to jeden z najpopularniejszych i stosunkowo łatwych sposobów wyprania cyfrowych wartości majątkowych. Uczestnicy transakcji pozostają anonimowi: nie podają swoich danych osobowych i lokalizacji, maskują używane numery IP oraz regulują zobowiązania kryptowalutą. Analiza płatności może co najwyżej wskazywać, że klient przeprowadza transakcje z adresami, które zostały powiązane z rynkami darknetu, ale dodatkowe stosowanie np. mikserów lub tokenów oferujących całkowitą anonimowość nie pozawala na powiązanie płatności z konkretnymi osobami. „Towar" dostarczany jest nabywcy standardowymi przesyłkami pocztowymi lub z wykorzystaniem usług kurierskich. Wynika z tego, że osoba zamawiająca w sieci np. narkotyki może odebrać je w paczkomacie lub w skrzynce na listy w dowolnej części globu.

Założycielem pierwszego, działającego na ogólnoświatową skalę darkmarketu o nazwie Silk Road był Ross Ulbricht. Funkcjonująca od 2011 r. platforma obsłużyła prawie 150 000 kupujących i 4000 sprzedawców, przede wszystkim ze Stanów Zjednoczonych. Oprócz samej witryny z ofertami i możliwości komunikowania się ze sprzedającym towar/usługę, użytkownicy Silk Road posiadali także dostęp do forum dyskusyjnego na temat używania narkotyków, realizacji płatności w BTC, wiarygodności poszczególnych dostawców itp. Strona nie służyła zatem tylko do transakcji, ale stanowiła ponadto cenne źródło informacji i wymiany poglądów dla globalnej społeczności cyberprzestępców. Dzięki temu relacje między nimi miały profesjonalny charakter, opierały się na zaufaniu i libertyńskich poglądach. W 2013 r., po likwidacji Silk Road, powstały nowe, podobne platformy i chociaż największe z nich są po niedługim czasie zamykane przez służby ochrony prawa, to zaraz potem pojawiają się kolejne darkmarkety.

> Silk Road działał do 2013 r., kiedy to FBI zlokalizowało serwer hostujący jego treści. Ross Ulbricht został aresztowany i skazany na karę dożywotniego pozbawienia wolności. Ujęcie podejrzanego miało specyficzny przebieg: agenci federalni obserwowali go od dłuższego czasu po to, aby w momencie zatrzymania nie zdążył zamknąć matrycy swojego laptopa i zaszyfrować dostępu do danych znajdujących się w pamięci urządzenia. Dread Pirate Roberts, bo taki był pseudonim Ulbrichta, za pomocą laptopa logował się do konta administratora Silk Road i komunikował z serwerem hostującym nielegalne treści. Komunikacja, podobnie jak autoryzacja użytkownika laptopa, były szyfrowane silnym kluczem kryptograficznym, a dostęp do niego umożliwiłby agentom przechwycenie danych mających decydujące znaczenie dla śledztwa (np. prywatnych kluczy szyfrujących). Ostatecznie udało się zatrzymać Rossa Ulbrichta w bibliotece w San Francisco z otwartym laptopem i poznać zawartość dysku.

Interesującym aspektem społeczności Silk Road był poziom koordynacji bitcoinowych transakcji. Z oczywistych względów użytkownicy darkmarketu chcą oddzielić wszelkie przesyłane dane od własnej tożsamości. Na Silk Road każdy sprzedawca miał własną metodę ukrywania i dostarczania produktów. Ponadto celem zawierania umowy sprzedaży na podobnych stronach kupujący muszą najpierw założyć własne konto i zdeponować na nim fundusze. Profesjonalnie zarządzane darkmarkety mają w swojej infrastrukturze wbudowane systemy „zaciemniania" źródła pochodzenia środków i ich dalszego przeznaczenia, np. Silk Road stosował wspomniane już „tumblery", które „mieszały" wszystkie płatności za pomocą złożonego algorytmu pozornych transakcji, co uniemożliwiało powiązanie środków zdeponowanych na platformie z BTC obsługującymi konkretną transakcję.

Crowdfunding

Crowdfunding, nazywany także finansowaniem społecznościowym, to zbieranie zazwyczaj stosunkowo niewielkich datków od wielu osób celem uzyskania kapitału na zaplanowane przedsięwzięcie. Wskazana aktywność odbywa się przy wykorzystaniu wirtualnych platform i dlatego duże znaczenie w crowdfundingu odgrywają media typu YouTube czy Twitter. Crowdfunding może być oparty na darowiznach *sensu stricte*, kiedy darczyńca nie spodziewa się zwrotu równowartości przekazanych środków ani żadnej innej rekompensaty. W innym scenariuszu crowdfunder wspiera finansowo projekt w oczekiwaniu na nagrodę w postaci np. dywidendy z wypracowanego zysku.

W przypadku prania pieniędzy najefektywniejszy dla przestępców jest crowdfunding w formie pożyczek scentralizowanych lub udzielanych w systemie peer-to-peer (P2P). W pierwszym przypadku crowdfunder pożycza pieniądze osobom fizycznym lub firmom w zamian za odsetki. Chociaż istnieją platformy ukierunkowane wyłącznie na pożyczki zorientowane społecznie, to większość działa w celach zarobkowych i konkuruje na rynku z innymi pośrednikami finansowymi. Przykład stanowi KIVA[29] oferująca kredyty w kwocie od 100 do 100 000 dolarów amerykańskich m.in. rolnikom i organizacjom pozarządowym. W opisanym systemie nie trudno wyobrazić sobie podmiot, którego budżet oparty jest na środkach pochodzących z nielegalnego źródła i pod przykrywką „ekonomii współdziałania" udziela internetowych pożyczek na korzystnych warunkach osobom aplikującym o wsparcie. Możliwość kontrolowania takich działań przez organy ochrony prawa zmniejsza się, jeśli do relacji pożyczkodawca-pożyczkobiorca dochodzi bezpośrednio w systemie P2P. Co prawda firmy pożyczkowe, pod względem przepisów prawa, posiadają status VASP, ale mogą doskonale kamuflować swoją działalność operując w jurysdykcjach o nieefektywnym systemie AML/CFT.

Wirtualne zbiórki crowdfundingowe wykorzystywane są przez organizacje neonazistowskie w Stanach Zjednoczonych. Oprócz kwestii praktycznych związanych z funkcjonowaniem walut cyfrowych, działający w Internecie ekstremiści używają kryptowalut, gdyż kojarzą się one z ideologią głęboko zakorzenionej nieufności wobec instytucji finansowych, jako rzekomo zarządzanych przez „światową finansjerę". Dodatkowo, do neonazistów przemawiają libertariańskie początki filozofii bitcoina połączone z buntem przeciwko „establishmentowi". Ponieważ amerykańscy neonaziści są rugowani z popularnych platform crowdfundingowych typu Patreon, opartych na zbiórkach pieniądza elektronicznego i przelewach bankowych, to tworzą alternatywne serwisy do dotacji w formie zdecentralizowanych tokenów. W taki sposób powstała strona o nazwie Hatreon: chociaż co jakiś czas firmy hostujące witrynę odmawiają jej utrzymywania, to Hatreon pojawia się ponownie korzystając z nowej domeny lepiej maskującej administratora. Zbiórka kryptowalut prowadzona jest także na internetowej stronie „The Daily Stormer". Znajduje się tam dokładna instrukcja w jaki sposób realizować przelewy kryptowalutowe na rzecz skrajnie prawicowych aktywistów. Podobnie działania rekrutacyjne dżihadystów w Internecie są często ściśle powiązane z apelami o pomoc finansową dla terrorystów opartą na crowdfundingu.

Initial Coin Offering

Kolejna metoda pozwalająca na wypranie pieniędzy, wykorzystuje instytucję *Initial Coin Offering* (ICO). W większości przypadków w ICO chodzi o gromadzenie kapitału na wdrożenie innowacyjnego projektu przez małe, pozbawione większego kapitału firmy. Organizują one emisję tokenów: inwestor, przy wykorzystaniu odpowiednich aplikacji, kupuje cyfrowe żetony płacąc za nie kryptowalutą lub pieniądzem elektronicznym. W ten sposób powstają „inteligentne umowy", jako algorytmy komputerowe, funkcjonujące w oparciu o technologię blockchain, przechowujące i realizujące warunki kontraktu za pomocą samorealizującej się instrukcji. Nieodłączny element ICO stanowi tzw. biała księga (ang. *white paper*) zawierająca szczegółowy opis projektu celem zachęcenia inwestorów do wyłożenia pieniędzy na jego realizację. Całość przedsięwzięcia promowana jest w mediach społecznościowych typu Instagram, Facebook, YouTube i Twitter. Budowane są też specjalne strony internetowe w ramach kampanii ICO oraz platformy ułatwiające potencjalnym inwestorom odnajdywanie ofert (np. Tokenmarket, ICO Bazaar). Z założenia uzyskane w ten sposób fundusze wykorzystuje się do wdrożenia pomysłu oraz samozatrudnienia członków start-upu, wynajęcia biura itp.

> Michael Stollery vel Michael Stollaire, nazywany „Ewangelistą Blockchaina", w ramach spółki Titanium Blockchain Infrastructure Services wyemitował w ramach ICO w 2017 r. tokeny o nazwie BAR i sprzeniewierzył otrzymane w ten sposób od inwestorów 21 mln dolarów. W opublikowanym wcześniej *white paper* Stollery obiecał utworzenie globalnego ekosystemu wymiany dóbr i usług opartego na blockchainie oraz walutę BAR, a także składał fałszywe oświadczenia o współpracy z Apple i IBM. Inne zarzuty SEC postawione Stollery to wprowadzanie w błąd inwestorów i pomijanie istotnych faktów dotyczących realizowanego projektu, rozpowszechnianie nieprawdziwych informacji o kapitałowym powiązaniu Titanium Blockchain z FED oraz notowaniach tokenów BAR na giełdach kryptowalutowych. Ostatecznie nie powstał żaden produkt oferowany w ramach Titanium Blockchain, a zebrane środki oszust włączył do prywatnego majątku i przeznaczył na cele konsumpcyjne. Podobnych, oszukańczych ICO było więcej np. Crypto Asset Management i Timothy Enneking, Plexcorps i Dominic Lacroix czy Sabrina Paradis-Royer.

Kapitalizacja światowego rynku tokenów cyfrowych szacowana jest w miliardach dolarów, a ich wartość oraz liczba programów opartych na ICO i *smart contracts* stale rośnie. W rzeczywistości nominalna wartość funduszy zebranych w ramach ICO może być bardzo myląca z wielu powodów np. dotyczyć żetonów o formalnie dużym potencjale kapitalizacji, ale funkcjonujących na niszowej giełdzie. Istnieją ponadto sposoby sztucznego generowania tokenowych transakcji (np. wykorzystując boty) i „nakręcanie" ich podaży i popytu

29 http://www.Kiva.org, data odczytu: 23.08.2019 r.

(oszustwo „pump and dump"). Programy typu *smart contract* narażone są ponadto na działanie praw rynku, a więc wahania kursu, nietrafione inwestycje, czy niekompetencję zespołu realizującego projekt. Wszystko to powoduje, że duża część projektów typu ICO w ogóle nie dochodzi do skutku. Amerykańska SEC, a za nią policja i prokuratura, w ostatnich latach prowadziła postępowania przeciwko wielu malwersantom finansowym wykorzystującym formułę ICO do oszukania inwestorów. Ogólny schemat działania przestępców polegał na składaniu obietnic nierealnie wysokich zysków dla kupujących tokeny, które ostatecznie okazywały się nic nie warte.

Oprócz działań stanowiących umyślne przestępstwo oszustwa, pojawiają się przypadki nieświadomego, ale jednak niezgodnego z prawem zarządzania tokenami cyfrowymi, bowiem wieloraka postać cyfrowych praw majątkowych generuje problemy z ich zakwalifikowaniem pod względem prawno-ekonomicznym. W Stanach Zjednoczonych SEC od 2017 r. proceduje przeciwko emitentom tokenów cyfrowych, którzy nie uzyskali stosownych zgód na emisję lub nie zarejestrowali swojej działalności, ponieważ w rozumieniu tamtejszego prawa tokeny cyfrowe mogą być papierami wartościowymi. Przykładem jest sprawa Zachary Coburna. W okresie lipiec 2016 r. – listopad 2017 r. założył on i prowadził bez zezwolenia platformę tradingową o nazwie EtherDelta.

Użytkownicy EtherDelta za pomocą łatwego w obsłudze interfejsu, przypominającego internetowe platformy obrotu papierami wartościowymi, składali zlecenia kupna/sprzedaży dowolnego tokena standardu ERC20. Kontrahent podawał symbol tokena, proponowaną cenę w ether i czas obowiązywania oferty (mierzony w „blokach"). Operacje biznesowe oparto na algorytmie „inteligentnych umów" działających na Blockchain Ethereum, dzięki czemu osoby zainteresowane mogły wchodzić między sobą w bezpośrednie relacje. EtherDelta była dostępna dla każdego użytkownika sieci przez 24 godziny na dobę, siedem dni w tygodniu, a opłata dla jej administratora wynosiła 0,3% ceny transakcji. W okresie gdy Coburn był właścicielem platformy przyjęła ona ponad 3,6 miliona zleceń, które zgodnie z SEC stanowiły obrót papierami wartościowymi. W Komisji nie zarejestrowano jednak EtherDelta jako krajowej giełdy papierów wartościowych i SEC nałożyła na Coburna karę 300 tys. dolarów[30].

30 *Securities and Exchange Commission v. Zachary Coburn*, https://www.sec.gov/litigation/admin/2018/34-84553.pdf, data odczytu: 23.08.2019 r.

Platformy typu P2P

Platformy P2P oferują usługi wymiany wartości majątkowych w formie cyfrowej na inne lub takie same tokeny, albo konwersję pieniądza elektronicznego na waluty cyfrowe oraz walut cyfrowych na pieniądz bankowy. Mają one zazwyczaj postać witryn internetowych, ułatwiających komunikację między osobami zainteresowanymi zawarciem umowy. Do wymiany dochodzi bezpośrednio między dwoma podmiotami, które wcześniej ustaliły między sobą szczegóły transakcji. Innym razem zainteresowani wystawiają swoje oferty określając cenę kupna/sprzedaży tokenu, a specjalne oprogramowanie automatycznie realizuje kontrakt według ustalonych parametrów. Omawiane serwisy będą zasadniczo objęte definicją *Virtual Asset Service Provider*. Wątpliwości powstają, kiedy system umożliwia tylko zamieszczanie ogłoszeń dotyczących kupna/sprzedaży VA i udostępnia komunikator (chat) stronom przyszłej transakcji, ale nie hostuje narzędzi (np. portfeli) pozwalających na jej przeprowadzenie. Opisany podmiot może nie podlegać definicji VASP, jeśli nie uczestniczy bezpośrednio w transferach walut wirtualnych i nie pobiera z tego tytułu żadnych opłat i prowizji[31].

W kwietniu 2019 r. FinCEN ukarał Erica Powersa grzywną 35 350 dolarów za to, że nie zarejestrował swojej działalności u regulatora jako przedsiębiorca świadczący usługi pieniężne i nie zgłosił do FinCEN „podejrzanych" transakcji walutowych. Powers kupował i sprzedawał bitcoiny „z ręki do ręki" lub za pośrednictwem poczty (przeprowadził np. 160 zakupów BTC realizując osobiście transakcje gotówkowe w miejscach publicznych z osobą poznaną na kryptowalutowym forum). Koordynował także przelewy bankowe z poziomu darknetu obsługując swoich klientów w sieci TOR. Mężczyzna nie podejmował żadnych prób ustalenia tożsamości swoich kontrahentów i źródła pochodzenia jednostek kryptowaluty oraz nie powiadomił organów nadzoru nad rynkiem finansowym o swojej działalności[32].

Serwisy P2P, chociaż powinny spełniać obowiązki nałożone na VASP, to często działają poza jakąkolwiek kontrolą, a swoje usługi reklamują w darknecie na forach internetowych, w mediach społecznościowych lub pocztą pantoflową. Najbardziej profesjonalne z nich noszą nazwę „mikserów" i „tumblers". W pierwszym przypadku chodzi o płatną usługę, zarządzaną przez administratora serwisu, polegającą na

31 *Virtual Assets and Virtual Asset Service Providers*..., op. cit., s. 15.

32 *FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws*, April 18, 2019, https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money, data odczytu: 23.08.2019 r.

wysłaniu na jeden adres jednostek kryptowaluty i „wymieszaniu" ich z innymi jednostkami ulokowanymi pod tym samym adresem. W rezultacie przestępca otrzymuje z powrotem identyczną liczbę bitmonet, ale każda z nich ma inną, od kryptowaluty pochodzącej bezpośrednio z przestępstwa, historię w łańcuchu bloków. Kolejnym sposobem wyprania cyfrowych jednostek są zdecentralizowane, autonomiczne platformy peer-to-peer typu tumblers, na których osoby zainteresowane „zmiksowaniem" posiadanych tokenów same organizują się, wpłacają bitmonety, a następnie wypłacają liczbowo identyczną, ale jakościowo różną pulę jednostek. Instytucje finansowe mogą zidentyfikować nielegalną wymianę typu P2P poprzez śledzenie aktywności tzw. kont lejkowych (ang. *funnel account*), na które wiele osób wpłaca pochodzące z czynów niedozwolonych środki w celu ich „wyprania". Cyberprzestępcy wykorzystują ponadto „muły" do przeprowadzania transakcji, której podstawione osoby nie są rzeczywistymi beneficjentami. „Muł" może być nieświadomy, że uczestniczy w praniu pieniędzy, jednak zazwyczaj zdaje sobie sprawę z nielegalnego charakteru realizowanych transferów, a nawet działa w wieloosobowych grupach piorących pieniądze na dużą skalę[33].

Bankomaty kryptowalutowe

Bankomaty kryptowalutowe (ang. *CVC kiosks*, *bitcoin Automated Teller Machines*) działają podobnie jak tradycyjne bankomaty przeznaczone do obsługi pieniądza elektronicznego i wypłaty gotówki, ale w tym przypadku chodzi o przesyłanie środków między wirtualną giełdą a portfelem klienta. Niekiedy maszyny same działają jak taka giełda i mogą łączyć się online z platformami zamkniętymi, administrowanymi przez właścicieli *CVC kiosks*. W praktyce terminale najczęściej wykorzystywane są do przyjmowania walut wirtualnych od klienta i wypłacania w zamian pieniędzy lub odwrotnie, konwersji pieniądza fiducjarnego (w formie gotówki lub elektronicznej) na kryptowalutę. Dostępna jest także opcja przesyłania bitmonet z jednego adresu na inny adres. Mapa lokalizacji kryptobankomatów na świecie znajduje się na stronie Bitcoin ATM Map[34] (w Polsce w połowie 2019 r. zaznaczono 56 takich maszyn, chociaż zapewne funkcjonowało ich więcej).

Bankomaty kryptowalutowe należy kwalifikować jako VASP. FinCEN opublikował wytyczne wyjaśniające, że właściciel/operator bankomatów łączących posiadacza rachunku bankowego z jego rachunkiem na giełdzie kryptowalutowej, musi wypełniać obowiązki nałożone na dostarczycieli usług związanych z walutami cyfrowymi odnośnie procedur transakcyjnych. Wyjątkowo, jeśli kiosk ma tylko funkcję sprawdzania salda portfela oraz wypłacania bitmonet, to nie podlega reżimowi VASP. Zasadniczo jednak właściciele kiosków CVC w Stanach Zjednoczonych, którzy przyjmują i przekazują wartości majątkowe, muszą przestrzegać przepisów FinCEN regulujących operacje pieniężne[35].

Kryptobankomaty, podobnie, jak każdy inny VASP, także są wykorzystywane do prania pieniędzy. Zarówno fundamentaliści islamscy, jak i neonaziści reklamują sposoby finansowania ich organizacji z wykorzystaniem kiosków CVC. W mediach społecznościowych zamieszczono instrukcje, jak krok po kroku wymienić za pomocą maszyny pieniądz fiducjarny na kryptowalutę i przelać środki na adres organizacji ekstremistycznej, a linki do takich stron, jak wspomniana Bitcoin ATM Map, pokazują potencjalnemu darczyńcy lokalizację najbliższego kryptobankomatu. Darczyńca przy zachowaniu reguł ostrożności może całkowicie anonimowo zrealizować przekaz. Chociaż niektórzy operatorzy kiosków zarejestrowali swoją działalność i wdrożyli reguły AML, to jednak większość z nich działa poza wszelkimi regulacjami – operatorzy nie gromadzą informacji o klientach i nie identyfikują źródła pochodzenia środków[36].

> W sprawie „CVC Kiosks – Khalil Wright" z roku 2017 amerykański sąd dla okręgu Maryland skazał Khalila Wrighta na dwa lata pozbawienia wolności za „posiadanie z zamiarem dystrybucji kontrolowanej substancji". W trakcie dochodzenia ustalono, że Wright zakupił BTC za co najmniej 112 797 USD w bankomacie w Baltimore i wysłał je bezpośrednio na adres darkmarketu AlphaBay, jako zapłatę za narkotyki[37].

WNIOSKI

Przestępcy będą coraz powszechniej wykorzystywać cyfrowe wartości majątkowe i wirtualne serwisy do prania pieniędzy i finansowania terroryzmu; świadczą o tym następujące fakty:

1. racjonalna i powszechnie uznana koncepcja cyklu życia technologii wg Gartnera pokazuje, że blockchain i powiązane z nim waluty cyfrowe znajdują się na tzw. płaskowyżu produktywności, a więc technologia ta dojrzała do powszechnego zastosowania. Przedsiębiorstwa coraz częściej wdrażają różnego rodzaju projekty oparte na blockchainie i rośnie liczba użytkowników VA oraz VASP. Skutkuje to nowymi formami przestępczości ukierunkowanymi na tokeny cyfrowe;

33 *Advisory on Illicit Activity Involving Convertible Virtual Currency*..., op. cit., s. 5.

34 Bitcoin ATM Map, https://coinatmradar.com/bitcoin-atm-map/, data odczytu: 23.08.2019 r.

35 *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencie*, FIN-2019-G001 Issued: May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf, data odczytu: 23.08.2019 r.

36 Tamże, s. 7.

37 *Advisory on Illicit Activity Involving Convertible Virtual Currency*..., op. cit., s. 7.

2. przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu z wykorzystaniem VA i VASP oraz zwalczanie tego typu przestępczości jest bardzo trudne ponieważ funkcjonują specjalistyczne narzędzia teleinformatyczne anonimizujące ruch sieciowy, sprawcy mają dostęp do globalnej sieci, poszczególne kraje charakteryzują różne, często bardzo odmienne regulacje dotyczące tokenów cyfrowych, a mechanizmy międzynarodowej pomocy prawnej są zbyt mało efektywne;

3. nawet w takich państwach jak Polska, które w pełni implementowały do porządku prawnego rekomendacje FATF w zakresie AML/CFT realizacja efektywnego nadzoru nad wirtualnym rynkiem jest trudna, a niekiedy wręcz iluzoryczna. Przykład stanowią platformy tradingowe zarejestrowane w „egzotycznych" jurysdykcjach, ale dostępne dla wszystkich użytkowników Internetu;

4. wiarygodne, opisane w niniejszej pracy, źródła wskazują, że w wirtualne pranie pieniędzy zaangażowane są miliardy dolarów na całym świecie. W przypadku finansowania terroryzmu to kwoty nieporównywalnie mniejsze, gdyż ekstremiści dopiero testują nowe technologie i uczą się je wykorzystywać.

Ustalony w ten sposób stan faktyczny wymaga podjęcia przez szeroko rozumiane instytucje ochrony prawa skutecznych działań przeciwko praniu pieniędzy i finansowaniu terroryzmu tokenami cyfrowymi. Chodzi o analizę charakteru prawnego, ekonomicznego i technicznego VA i VASP, edukację w tym zakresie, krajowe partnerstwo publiczno-prywatne i kooperację międzynarodową w walce z cyberprzestępczością. W Polsce powinna zostać zacieśniona współpraca pomiędzy organami ścigania przestępstw, Komisją Nadzoru Finansowego i Generalnym Inspektorem Informacji Finansowej celem efektywniejszego rozpoznawania i przeciwdziałania zagrożeniom. Jeśli chodzi o polską Prokuraturę, to obecnie walka z nadużyciami w cyberprzestrzeni jest jednym z priorytetów jej funkcjonowania, a liczne, pozytywne działania w tym zakresie opisano w dokumencie *Wyzwania i sukcesy – Prokuratura 2019*[38]. Wciąż pozostaje jeszcze ogrom pracy do wykonania celem wypracowania jak najlepszego systemu do walki z nadużyciami w cyberprzestrzeni. W gruncie rzeczy jest to nieustanny proces dostosowywania się do nowych wyzwań. Gwarancję sukcesu daje tylko połączenie woli, zasobów i środków wszystkich działających w dobrej wierze uczestników rynku walut cyfrowych.

W przygotowaniu znajduje się monografia autora dotycząca opisywanego tematu pt. „Wykorzystanie walut i serwisów wirtualnych do prania pieniędzy i finansowania terroryzmu".

38 *Wyzwania i Sukcesy Prokuratura 2019*, https://pk.gov.pl/wp-content/uploads/2019/08/PROKURATURA-2019-1.pdf, data odczytu: 17.09.2019 r.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki jest niezależnym, pozarządowym instytutem naukowo-badawczym (Think Tank) o charakterze non profit, założonym w 2000 r. Misją Instytutu Kościuszki jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski jako aktywnego członka Unii Europejskiej oraz partnera sojuszu euroatlantyckiego. Instytut Kościuszki pragnie być liderem pozytywnych przemian, tworzyć i przekazywać najlepsze rozwiązania, również na rzecz sąsiadujących krajów budujących państwo prawa, społeczeństwo obywatelskie i gospodarkę wolnorynkową.

Instytut Kościuszki jest organizatorem Europejskiego Forum Cyberbezpieczeństwa CYBERSEC oraz Polskiego Forum Cyberbezpieczeństwa – pierwszych w Polsce oraz jednych z nielicznych w Europie corocznych konferencji poświęconych strategicznym wyzwaniom płynącym z cyberprzestrzeni i dotyczących cyberbezpieczeństwa. Więcej: http://cybersecforum.eu/.

Instytut Kościuszki jest wydawcą „European Cybersecurity Journal" (ECJ). ECJ to anglojęzyczny kwartalnik ekspercki poświęcony cyberbezpieczeństwu. Zawiera artykuły wiodących analityków i liderów opinii, ekskluzywne wywiady z decydentami oraz monitoring regulacji dotyczących kluczowych aspektów związanych z cyberprzestrzenią. Więcej: http://cybersecforum.eu/czym-jest-ecj/.

Biuro w Krakowie: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24,
www.ik.org.pl, e-mail: instytut@ik.org.pl